Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

Elektronické volby

Dan Valeček

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Dan Valeček

Informatika

Název práce

Elektronické volby

Název anglicky

Electronic elections

Cíle práce

Bakalářská práce je tematicky zaměřená na problematiku elektronických voleb (e-volby). Hlavním cílem bakalářské práce je charakterizovat problematiku e-voleb z pohledu technického řešení, bezpečnosti a transparentnosti. Dílčí cíle bakalářské práce jsou:
- charakterizovat princip a standardy e-voleb
- analyzovat metody e-voleb v zahraničí
- definovat nutná východiska pro zavedení v ČR

Metodika

Metodika řešené problematiky bakalářské práce je založena na studiu a analýze odborných informačních zdrojů. Praktická část práce je zaměřená na vypracování analytické studie řešení problematiky e-voleb. Na základě syntézy teoretických poznatků a výsledku vlastního řešení budou formulovány závěry bakalářské práce.

Doporučený rozsah práce

40 – 50 stránek

Klíčová slova

Elektronické volby (e-volby), eGovernment (e-Government), bezpečnost, technické řešení, legislativa, transparentnost

---

Doporučené zdroje informací

Computer science and software techniques in 2011. Vsetín: Silhavy, 2011. OpenPublish book series. ISBN 978-80-904741-0-9.

HERRNSON, Paul S. Voting technology: the not-so-simple act of casting a ballot. Washington, D.C.: Brookings Institution Press, c2008, ISBN 978-0-8157-3564-9.

Realities of E-voting Security. [on-line]. ISSN 1540-7993

Předběžný termín obhajoby

2015/16 LS – PEF

Vedoucí práce

Ing. Jan Jarolímek, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 28. 10. 2015

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 10. 11. 2015

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 14. 03. 2016

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Elektronické volby“ jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 14.3.2016 _____

Poděkování

Rád bych touto cestou poděkoval Ing. Jan Jarolímek, Ph.D za odborné konzultace v průběhu tvorby mé práce.

Elektronické volby

Souhrn

Tato práce je zaměřená na analýzu problematiky a dostupná řešení elektronických voleb a jejich přínosů pro uživatele a provozovatele. Problematika elektronických voleb je zcela jistě součástí neodvratné elektronizace státní správy a je tak budoucností volebního procesu. Informační technologie jsou už řadu let na stálém vzestupu a je třeba vyvíjet úsilí k dosažení a využití plného potenciálu těchto technologii. Přizpůsobováním technologií určitým standardům a principům tak vznikají systémy, které jsou za splnění nutných podmínek bezpečné a transparentní. Národní státy elektronické volební systémy zavádí ve snaze zvýšit volební účast. Hlavní výhodou internetového volebního procesu je možnost přihlášení se z různých prostředí a v různém čase. Uživatel je schopen se přihlásit z různých chytrých zařízení a to za splnění základní podmínky připojení k internetu. Tato práce má za cíl přednést širší pohled na problematiku elektronických voleb, zkušenosti ze zahraniční a návrh postupu elektronizace voleb v České republice.

Klíčová slova: Elektronické volby (e-volby), eGovernment (e-Government), Bezpečnost, Technické řešení, Legislativa, Transparentnost, Kryptografické šifry, Bezpečné procesy,

Electronic Elections

Summary

This work is focused on analysis and the possible solutions of electronic elections and their benefits to users and operators. The issue of electronic elections is certainly inevitable part of the computerization of the state administration and thus a future of electoral process. Information technologies are on a constant rise for a number of years and efforts must be made to achieve and utilize the full potential of new technologies. Adapting new technologies to certain standards and principles creates systems that meet the necessary safety a transparency conditions. Nation states introduced electronic voting systems in an effort to increase turnout. The main advantage of e-voting electoral process is the ability to log in from different environments and at different times. The user is able to log in from a variety of smart devices under the basic condition of the internet access. This work aims to give a broader perspective on the issue of electronic elections, the experiences from foreign countries and a proposal for the computerization of electoral process in the Czech Republic.

Keywords: Electronic elections (e-voting), eGovernment (e-Government), Security, Transparency, Legislation, Safe processes, Technical solutions, cryptographic ciphers

Obsah

Seznam obrázků

Seznam tabulek

1 Úvod

Téma elektronických voleb představuje zajímavé a aktuální téma. Hlavní důvod zavedení e-voleb ve všech státech, Českou republikou nevyjímaje, je dosažení větší volební účasti v době jejího neustálého poklesu a při správném řešení by mohla vést i k úspoře finančních prostředků. Užití nových technologií by mělo mít za následek větší atraktivitu a dostupnost voleb ze strany voličů. Strana autorit by měla také zaznamenat úbytek tlaku na zaměstnance státní správy v době voleb, ale hlavně zrychlení procesu sčítání a interpretace výsledků voleb.

V rešerši své práce bych se rád věnoval realizací řešení e-voleb. Jako hlavní teoretická východiska jsem si určil čtyři základní části. První část se zaměří převážně na legislativu a druhy voleb, které se konají v České republice. Druhá část představuje transparentnost, což je oblast, ve které je zapotřebí stanovit jasná pravidla ověřitelnosti volebního systému. Ve třetí části se zabývám zajištěním bezpečnosti voleb a jejich procesů. V čtvrté části popisuji možné technické řešení volebního systému.

Dále v analytické části této práce se pokusím analyzovat systémy e-voleb v zahraničí z vybraných států Evropy. Nastřádané informace mi pomohou ke stanovení kritérií a následné ohodnocení jednotlivých systémů. Ohodnocené systémy porovnám metodou párového porovnání alternativ a interpretuji výsledky. V závěrečné diskusi stanovím formou odpovědí na poležené otázky východiska pro možné zavedení e-voleb v České republice. Tato východiska vyložím a popíši v závěru.

2 Cíl práce a metodika

Bakalářská práce je tematicky zaměřená na problematiku elektronických voleb (e-volby). Hlavním cílem bakalářské práce je charakterizovat problematiku e-voleb z pohledu technického řešení, bezpečnosti a transparentnosti.

Mezi dílčí cíle bakalářské práce patří charakteristika principů a standardů e-voleb, které musí být v souladu s platnou legislativou v České republice dodrženy za účelem zachování možnosti ověření volby, soukromí voliče, férovost a transparentnosti voleb.

Dalším cílem je navrhnout takový model, u něhož bude možné zajistit pomocí kombinace kryptografických šifer a bezpečných procesů právě výše uvedené standardy.

Posledním dílčím cílem mé práce je analýza systémů e-voleb v zahraničí a následně definovat nutná východiska elektronizace voleb v České republice.

Metodika řešené problematiky bakalářské práce je založena na studiu a analýze odborných informačních zdrojů. Veškeré použité zdroje jsou volně dostupné, ověřitelné a jsou uvedeny v seznamu zdrojů na konci této práce.

V praktické části práce se věnuji vypracování analytické studie řešení problematiky systémů e-voleb v zahraničí. Analyzované systémy mezi sebou porovnám za využití metody párového porovnání. Stanovení váhy jednotlivých kritérií jsem realizoval za pomoci Saatyho metody.

Na základě syntézy teoretických poznatků a výsledků vlastního šetření budu formulovat závěry bakalářské práce.

3 Teoretická východiska

3.1 Legislativa

3.1.1 Volební právo a jeho základní principy

Volby jsou jedním ze základních nástrojů demokracie a demokratického státního zřízení, zaručují svobodnou soutěž politických stran a vyjádření vůle většiny skrze veřejná hlasování. Volby jsou zdrojem legitimity veškerých státních orgánů České republiky jakožto hlavního institutu nepřímé, tzv. zastupitelské demokracie. Z hlediska práva rozlišujeme volební právo v subjektivním a objektivním smyslu. Volební právo v objektivním smyslu je vnímáno jako soubor právních norem upravujících přípravu, organizaci a provádění voleb. Zatímco za volební právo v subjektivním smyslu považujeme právo oprávněných voličů (občanů) účastnit se formování orgánů veřejné moci skrze veřejná hlasování, a to jak pasivně (být volen), tak aktivně (volit své zástupce do státních orgánů). [16]

Dalším důležitým atributem svobodných demokratických voleb jsou tzv. volební principy, představující souhrn esenciálních požadavků a podmínek, jejichž dodržení je nezbytným předpokladem prováděných voleb. Mezi základní principy voleb řadíme:

I. Všeobecné volební právo. Podstatou všeobecného volebního práva je určení okruhu oprávněných účastníků voleb a podmínek, při jejichž dodržení mají oprávnění účastníci právo volit své zástupce (aktivní složka volebního práva) a ucházet se o zvolení (pasivní složka volebního práva). Na tomto místě je důležité podotknout, že princip všeobecného volebního práva nezaručuje, že právo účastnit se voleb má každý občan bez výjimky.
II. Rovné volební právo. Oprávnění voliči, kterým nebrání ve výkonu volebního práva zákonná překážka, se účastní voleb za stejných podmínek. Voliči mají mít zaručeny rovné podmínky a zacházení ve všech stádiích volebního procesu.
III. Přímé volby. Voliči hlasují bezprostředně pro navržené kandidáty. Princip přímých voleb má zajistit bezprostřední vztah mezi hlasováním voliče a výsledným obsazením mandátu.

IV. Tajné hlasování. Volby musí proběhnout způsobem znemožňujícím určit, jak určitý volič hlasoval. Tento princip je zaručován jak samotným průběhem hlasování (volič se musí povinně odebrat hlasovat za plentu, v opačném případě mu okrsková volební komise neumožní hlasovat), tak samotným volebním lístkem, ze kterého není možné identifikovat konkrétního voliče.

V. Svobodné volby. Za svobodné volby lze považovat takové volby, v nichž existuje svoboda ucházet se o hlasy a podporu voličů ve volebním procesu, svoboda zakládání politických stran a svoboda navrhování kandidátů, svoboda komunikace s veřejností, svoboda voličů vybírat si z více alternativ ve volebním procesu.

Kromě výše uvedených základních volebních principů lze dále řadit mezi volební principy například princip volebního období, kdy úspěšní kandidáti jsou ustavováni do funkcí na předem zákonem určený čas. [17]

3.1.2 Volební systém v České republice

Volební systém definuje způsob, jakým jsou přidělovány kandidátům mandáty s ohledem na výsledky hlasování ve volbách. Výše uvedená definice není ovšem jedinou, lze se setkat například s definicí, kdy volební systém představuje pravidla, pomocí kterých se na základě počtu hlasů rozdělují ve volbách mandáty mezi strany či jednotlivé kandidáty. V širším pojetí lze konstatovat, že volební systém zahrnuje rozsáhlý proces voleb od vyhlášení voleb a přípravy volebního procesu, přes samotné provádění a průběh veřejného hlasování až po vyhlášení výsledků. Mezi základní dva volební systémy řadíme poměrný volební systém a většinový volební systém, přičemž oba dva výše uvedené systémy jsou na území České republiky k dnešnímu dni využívány. [16]

V poměrném volebním systému se mandáty rozdělují v určitém poměru k počtu získaných hlasů, volební území je rozděleno na více mandátové volební obvody. V České republice je tento systém aplikován ve volbách do Poslanecké sněmovny Parlamentu České republiky, ve volbách do zastupitelstev obcí a krajů a v poslední řadě ve volbách do Evropského parlamentu. Zde si dovolím upozornit na tzv. pětiprocentní omezovací klauzuli, která je využívána u poměrného volebního systému v ČR. Tato klauzule zamezuje jakémukoli subjektu, pasivně se účastnícího výše uvedených voleb, být zvolen,

pokud nepřekročí hranici 5 % obdržených hlasů ve volbách. Otázkou, zda je tato omezovací klauzule v rozporu (v předchozí kapitole uváděných zmíněných principů volebního práva), se již zabýval Ústavní soud České republiky a dospěl k závěru, že tato klauzule „*není v rozporu s charakteristikou volebního systému v ústavě či volebním zákonu jakožto poměrného zastoupení, jestliže a pokud tato opatření neomezují poměrné zastoupení podstatnou měrou. Demokratické státy zaváděly postupně systém poměrného zastoupení, opatřený pětiprocentní resp. tříprocentní klauzulí, aniž by tím považovaly princip poměrného zastoupení za znehodnocený"* [1].

Většinový volební systém je oproti poměrnému založen na principu „vítěz bere vše", kdy všechna křesla, do kterých jsou kandidáti voleni, získá vítěz voleb, přičemž volební území je rozděleno na jednomandátové volební obvody. Tento systém je uplatněn v České republice při volbách do Senátu Parlamentu České republiky. Vítěz ve většinových volbách musí přesáhnout hranici 50 % obdržených, z tohoto důvodu se až na výjimky volby dle většinového volebního systému uskutečňují ve dvou kolech, kdy do druhého kola postupují dva nejsilnější kandidáti.

3.1.3 Legislativní rámec voleb a volebního práva

Volební právo se řadí v demokratickém právním státě mezi základní lidská práva, je zaručeno jak na mezinárodní úrovni skrze mezinárodní smlouvy a úmluvy, tak na vnitrostátní úrovni skrze právní předpisy. Základní rámec je zaručen na úrovni ústavního práva, zejména ústavním zákonem č. 1/1993 Sb., Ústavou České republiky a ústavním zákonem č. 2/1993 Sb., Usnesení předsednictva České národní rady o vyhlášení LISTINY ZÁKLADNÍCH PRÁV A SVOBOD jako součástí ústavního pořádku České republiky (Listina základních práv a svobod).

Za nejdůležitější ustanovení Listiny základních práv a svobod pokládám článek 21:

I. Občané mají právo podílet se na správě veřejných věcí přímo nebo svobodnou volbou svých zástupců.
II. Volby se musí konat ve lhůtách nepřesahujících pravidelná volební období stanovená zákonem.
III. Volební právo je všeobecné a rovné a vykonává se tajným hlasováním. Podmínky výkonu volebního práva stanoví zákon.
IV. Občané mají za rovných podmínek přístup k voleným a jiným veřejným funkcím.

V souvislosti s volebním právem a volbami bych zmínil článek 17, článek 18, článek 19 a článek 102 Ústavy České republiky. [17] [18]

3.1.4 Obecně o volbách do Parlamentu České republiky

Volby vyhlašuje nejpozději 90 dní před jejich konáním prezident republiky s kontrasignací předsedy vlády. Volby se musí uskutečnit ve lhůtě počínající třicátým dnem před uplynutím končícího volebního období a končícím dnem jeho uplynutí. Volby se konají ve dvou po sobě následujících dnech a to vždy v pátek a sobotu, samotné hlasování probíhá ve stálých a zvláštních volebních okrscích. Oprávnění voliči jsou zapsáni na stálém či zvláštním voličském seznamu. [16]

3.1.5 Volby do Poslanecké sněmovny Parlamentu České republiky

Volby do Poslanecké sněmovny Parlamentu České republiky se konají dle zásad poměrného zastoupení, oprávnění voliči volí 200 poslanců na období čtyř let. Volebním územím je celá Česká republika, rozdělená na 14 volebních obvodů (území mimo ČR vymezena obvodem příslušného zastupitelského úřadu). Každé politické straně, koalici či hnutí je přidělen jeden hlasovací lístek. Při volbách je uplatněna uzavírací klauzule spolu s tzv. aditivní klauzulí (jedna politická stran či hnutí musí dosáhnout minimálně 5 % odevzdaných hlasů, koalice dvou hnutí již 10 % a takto se hranice zvyšuje až na 20 %). Pro přepočet hlasů na získané mandáty se užívá tzv. D'Hondtova metoda. [16]

3.1.6 Volby do Senátu Parlamentu České republiky

Volby do Senátu Parlamentu České republiky se konají podle zásad většinového volebního systému, je voleno 81 senátorů na volební období šesti let, přičemž každé dva roky se volí jedna třetina senátorů. Česká republika je pro účely voleb do senátu rozdělena na 81 volebních obvodů (velikost volebních obvodů není neměnná, v průběhu času dochází k proměnám založených na počtu obyvatel). Kandidují jednotliví občané, úspěšný kandidát musí získat přes 50 % odevzdaných hlasů v daném volebním obvodu, pokud takového kandidáta není, koná se druhé kolo voleb za účasti již pouze dvou nejúspěšnějších kandidátů z prvního kola. V případě zániku mandátu senátora v průběhu volebního období se konají doplňující volby. [16]

3.1.7 Volby do zastupitelstev obcí a krajů

Volby do zastupitelstev obcí a krajů se konají dle zásad poměrného zastoupení, přičemž volební období je čtyřleté. Obdobně jako volby do Parlamentu ČR volby vyhlašuje prezident republiky při dodržení stejných lhůt. Počet členů zastupitelstev se řídí počtem obyvatel příslušného kraje či obce. [18]

3.1.8 Volby do Evropského Parlamentu

Přistoupením ČR do Evropské unie se z občanů ČR stali též občané EU, čímž občanům ČR připadlo právo volit své zástupce ve volbách do Evropského parlamentu. Za ČR zasedá v současnosti v Evropském parlamentu 21 poslanců, tolik mandátů se ve volbách na území ČR přiděluje. Volebním obvodem je celá Česká republika. Evropští poslanci jsou voleni na období pěti let dle zásad poměrného zastoupení, při uplatnění uzavírací klauzule a D'Hondtovy metody přepočtu odevzdaných hlasů na mandáty. Z obecnějšího pohledu lze konstatovat, že volby do Evropského parlamentu jsou si v mnohém podobné s volbami do Parlamentu ČR. [18]

3.2 Transparentnost

3.2.1 Současný stav

V současné době si pod pojmem transparentnost voleb lze obecně představit několik různorodých věcí. Společností poslední dobou zejména hýbe otázka financování politických stran a hnutí, popřípadě jednotlivých kandidátů ucházejících se o zvolení. V tomto směru nejdále zachází úprava obsažená v zákoně o volbě prezidenta republika, upravující mimo jiné povinnost kandidátů vést transparentní účet (tzv. volební účet) a další některé povinnosti.[2]

V souvislosti s tématem této práce bych se rád věnoval zejména transparentnosti výsledků voleb, statistickým údajům a možnostem kontroly ze strany veřejnosti. Za současné situace nejvíce práce v tomto ohledu odvádí Český statistický úřad.

Český statistický úřad je jedním z volebních orgánů s působností ve věcech voleb a referenda a jako hlavní úkol má stanoveno „*vypracování závazného systému zjišťování a zpracování výsledků voleb, příp. výsledků hlasování v celostátním referendu, a zajištění vyhotovení příslušného programového vybavení pro účel zpracování a poskytování výsledků voleb a referenda“* [3].

V rámci plnění výše uvedeného cíle ČSÚ plní další úkoly, jako například zabezpečení technického systému zpracování výsledků voleb, zpracovává výsledky voleb, které následně zpřístupňuje, řeší stížnosti na funkci technických zařízení a programového vybavení a další. Vzhledem ke zmíněnému cíli a úkolům lze racionálně předpokládat, že Český statistický úřad by v případě e-voleb převzal důležitou úlohu, ne-li přímo primární a nejzásadnější.

K zajištění transparentnosti voleb, popřípadě celostátního referenda, shromažďuje ČSÚ pro volby zásadní údaje. V případě voleb do Poslanecké sněmovny shromažďuje ČSÚ následující údaje:

I. Jmenné seznamy a přehledy. ČSÚ shromažďuje seznamy všech platných kandidátů, zvolených poslanců, náhradníků a odvolaných kandidátů.
II. Celkové výsledky hlasování. Počet okrsků, voliči v seznamu, volební účast, odevzdané obálky, platné hlasy, procentuální míra platných hlasů.
III. Výsledky hlasování za volební kraje. Počty hlasů pro strany a počty hlasů pro strany v procentech.
IV. Výsledky hlasování za územní celky (dle krajů a okresů).
V. Územní přehledy o volební účasti (dle krajů a okresů).
VI. Rozdělení mandátů stranám. Počet platných hlasů, republikové mandátové číslo a počty krajských mandátů. Politické strany, politická hnutí a koalice postupující do skrutinia. Pořadí podílů hlasů, přehled zisku mandátů a přehled zisků mandátů v procentech.
VII. Informace o stavu zpracování.
VIII. Číselníky a registry (obcí a okrsků, kandidátních listin apod.)

Veškeré výše uvedené údaje jsou dostupné veřejnosti skrze internetové stránky ČSÚ, čímž je zajištěna možnost získat statistické údaje o volbách pro každého a kontroly ze strany veřejnosti. Údaje jsou průběžně zveřejňovány v době voleb a jsou dostupné po volbách.

3.2.2 Transparentnost e-voleb v České republice

Pro příklad E-voleb v České republice předpokládejme, že e-volby musí poskytnout nejméně stejnou úroveň transparentnosti voleb jako volby současné, spíše ovšem úroveň vyšší v několika směrech.

Co se týče institucionálního zajištění voleb, předpokládejme, že hlavní úlohu by mohl převzít Český statistický úřad, čímž by se rozšířila současná působnost. Z hlediska institucionálního se dle mého názoru jedná o vhodné řešení, jelikož ČSÚ disponuje zkušenostmi přímo z volebního procesu a také zajišťuje volby po technické a softwarové stránce.

K zajištění dostatečné úrovně transparentnosti volebního procesu musí e-volby umožňovat určité postupy a dosahovat jistých standardů, které jsou běžné pro „papírové“ volby. Pouze a jen volič může být schopen ověřit, zda a pro koho volil. Třetí osoba nesmí mít k takové informaci přístup (v opačném případě by došlo k porušení principu tajnosti volby). Provozovatel systému e-voleb musí být schopen ověřit součet přijatých hlasů a v případě potřeby být schopen odevzdané hlasy ověřitelným způsobem přepočítat. Provozovatel e-voleb musí mít úplný přehled o volbách včetně dat o odevzdaných hlasech a údaje o volbách musí po ukončení hlasování uveřejnit (tento postup již ČSÚ uplatňuje). Povinnost provozovatele e-voleb uveřejnit data o volbách se uplatní až po ukončení hlasování, žádná průběžná data či výsledky nesmí provozovat do uzavření hlasování uveřejnit (porušení této povinnosti může vést k narušení férovosti voleb a následné nutnosti volby opakovat).

Transparentnost voleb je nezbytným prvkem procesu voleb v demokratickém právním státě a spolu s dalšími prvky zajišťuje legitimitu voleb.

3.3 Bezpečnost

V demokratické zemi jsou volby jeden z nejdůležitějších nástrojů, jak mohou občané vyjádřit svoji vůli a názor. V mnoha demokratických zemích byl zaznamenán v posledních letech značný procentuální pokles ve statistikách volebních účastí, ať už se jednalo o volby parlamentní, senátní, do krajských či obecních zastupitelstev nebo o lidová hlasování (referenda). Elektronické volby otevírají voličům nové možnosti jak se zúčastnit voleb bezpečně na dálku přes internet. Bohužel je tady vždy určitá malá šance, že E-voting systémy mohou být napadeny nebo sabotovány, a proto se v této kapitole budu zabývat bezpečností takovýchto systémů.

Elektronické volby umožňují pohodlně lidem posílat své hlasy z různých míst a zařízení, ať už se nacházejí doma, v práci, na cestě nebo kdekoliv, kde mají internetové připojení. Navzdory tomu jak moc pohodlné e-volby jsou, je potřeba zajistit základní bezpečné procesy, zahrnující mimo jiné registraci voliče, ověření identity voliče, proces volby, proces sčítání a interpretaci výsledků. U veškerých těchto metod musíme zajistit 3 základní podmínky.

3.3.1 Soukromí

K zajištění soukromí voliče použijeme šifru blind signature, jež je založená na podstatě RSA šifry, která ovšem v určitých případech může být navzdory všem snahám, a to i za použití blind signature, prolomena. Za účelem zajištění soukromí voliče by systémy, používající výše uvedenou šifru, měly dosahovat větších možností zabezpečení u id obálek, přičemž id obálky musí generovat více validátorů namísto pouze jednoho individuálního validátoru. Tímto by měla být zajištěna integrita systému a následně soukromí voliče. Každý z těchto validátorů generuje unikátní id obálky za použití pseudo-random generátoru čísel a žádný z těchto validátorů nezná kompletní obsah obálky voliče, což zajišťuje nemožnost propojení obsahu obálky (hlasu voliče) s id obálky.[4][7]

3.3.2 Ověření

Schopnost voliče ověřit, zda jeho hlas byl úspěšně přijat, dosáhneme tak, že po přijetí obálky validátor odešle zprávu voliči s údajem pro zkontrolování hlasu. Úspěšného zkontrolování, zda byl hlas voliče správně započten, dosáhneme tak, že po skončení sčítání hlasů jsou hlasy uveřejněny a interpretovány transparentní výsledky, které si volič může zkontrolovat pomocí přijaté zprávy od validátoru.

Každý si může ověřit, že všechny sečtené hlasy, jsou validní, čehož docílíme tak, že obálky s unikátním id jsou podepsány soukromím klíčem validátoru a veškeré tyto rozšifrované hlasy jsou sečteny a interpretovány. Použití více autoritativních metod a stupňů kontroly chrání před duplikováním nebo před jedinci se záměrem hlasovat víckrát než jednou. Je zapotřebí více stupňů kontroly s rozloženou působností. Pokud alespoň jedna z těchto kontrol bude pracovat správně, je ověřitelnost zajištěná.[5]

3.3.3 Férovost

Férovost voleb znamená, že žádný z voličů nesmí získat informace o průběhu voleb kromě svého vlastního hlasu do doby, kdy se spustí proces sčítání. Tyto informace o prozatímním výsledku sečtených hlasů by mohly mít negativní dopad na férovost voleb. Férovosti voleb docílíme za použití kryptografické metody secret sharing, kdy žádný z kolektorů nezná úplný obsah obálek voličů a tím zamezí únikům informaci o průběhu hlasování během voleb. Kolektory při sčítaní spolupracují, kompletují hlasy voličů a následně je zveřejňují.[6]

3.3.4 Kryptografické metody

RSA - blind signaure je forma digitálního podpisu opravňujícího podepisujícího podepsat dokument, aniž by znal obsah dokumentu. Bezpečnosti u této techniky je dosaženo ve chvíli, kdy ani jeden z podepisujících nezná obsahy zašifrovaných dokumentů. Podepisující by neměli znát ani pro koho podepsali tento dokument. Je to jedna z nejvíce používaných kryptografických šifer za účelem zajištění soukromí hlasu voliče. Blind signature zajistí ověření voliče a přitom neuveřejní obsah dokumentu.[4]

Nechť *(n, e)* je veřejný klíč podepisujícího a *(d)* je soukromý klíč. Odesílatel zprávy vygeneruje náhodné číslo r, pro které platí *(r, n) = 1* a odešle je podepisujícímu.
$B' = r^e B$, kde *B'* je blind message a *B* je prázdná obálka.
Podepisující podepíše *B'*.
$S' = B'^d$, kde S' je podpis B'.
Odesílatel přijme S' a provede unblind k získání *S* pro originální obálku *B*.
$S = S'r^{-1} = B^d$, kde B^d je rozšifrovaná obálka.

Secret sharing - hlavní idea tohoto mechanismu je sdílet tajemství *S* mezi *n* uživatelů, pro které platí, že alespoň *t* uživatelů dokáže dosáhnout S. Tento systém je založen *na* polynomické interpolaci, kde polynom je y = f(x) stupně t-1. Je unikátně definován podle t bodů (Xi,Yi) se vzdáleností Xi. Důvěryhodná strana T přiřazuje S uživatelům n. Každá množina t uživatelů, sdílejících stejné secret číslo, může dosáhnout S.[6]

T vybere primární $P > max (S, n)$, *a definuje* $a_0 = S$.
T vybere *t-1* náhodný koeficient $a_1, a_2, \ldots . a_{t-1}$ z jednotné distribuce čísel množině *[0; P]*, ta definuje náhodný polynom Z_p, $f(x) = \sum_{j=1}^{t-1} a_j x^i$
T vypočítává $S_i = f(i)$, $1 \leq i \leq n$ a bezpečně přenáší sdílený S_i uživateli P_i.

Každá skupina *t* nebo více uživatelů obsahuje stejné sdílené číslo. Jejich sdílení zajišťuje *t* body vzdálenosti $(x, y) = (i, S_i)$, které umožňují výpočet koeficientu a_i, $1 \leq j \leq t-1$ *podle* Lagrangeovi interpolace. Tajemství (secret) je sestaveno jako $f(0) = a0 = S$.

Pseudo-random generátor je kryptografický algoritmus používaný za účelem generování náhodně vznikajících čísel, známých pod označením pseudo-náhodná čísla. Lineární kongruentní generátor je založen na lineárním opakování. Je používán za účelem generovat náhodné id číslo obálky. Validátory generují určitou velikost pseudo-náhodných čísel, která se opakují v intervalech a všechna tato čísla jsou připojena k formuláři unikátní id obálky voliče.[7]

Vybereme čtyři čísla

M, modulus; $m>0$

A,multiplier; $0 \leq a < m$

C,incement; $0 \leq a < m$

X_o,začínající hodnota; $0 \leq X_0 < m$

Žádoucí sekvence náhodných čísel (X_n), $X_n=(aX_{n-1}+c)$, $n \geq 0$

3.3.5 Bezpečné procesy

Autority:

Administrátor: je do systému e-voleb zapojen v ověřování voličů, sběru osobních údajů, volení a sčítání. Voliči se musí dostavit na příslušný úřad k ověření a podání svých osobních údajů potřebných k jejich ověření online. Jednou ověřená osoba bude přidána do národní databáze, což mu umožní zúčastnit se e-voleb.

Registrátor: tito registrující voliči jsou jednotlivě ověřování a porovnávaní s národní databází registrovaných. Pouze registrovaným voličům bude umožněn přístup do systému.

Validátor: validátory jednotlivě ověřují obálky a přiřazují id. Ověřovatel je zodpovědný za ověření voliči zaslaných obálek během voleb.

Kolektor: pro naplnění férovosti voleb, sbírání a sčítání hlasů. Kolektor sbírá hlasy během voleb, ale sčítat začne až po uplynutí volebního procesu.

Voliči:

Interakce volič a administrátor: alespoň jednou za život osobně navštívit příslušný úřad a registrovat se. Může být spojena i s běžnými činnostmi jako výměna občanského průkazu či vyřízení cestovního pasu.

Interakce volič a registrátor: před začátkem každých voleb by se voliči měli zapsat do voleb.

Zpětná vazba Registrátor: Pouze ověření zapsaní voliči obdrží prostřednictvím datové schránky přihlašovací údaje k volbám.

Interakce volič a validátor: Ověření voliči vyplní formulář, jenž je oslepen (blinded) a odeslán validátoru na ověření.

Zpětná vazba validátora: validátor podepíše příchozí obálku soukromým klíčem za účelem zjištění adresáta a poté odešle zprávu voliči o přijetí hlasu spolu s klíčem pro zkontrolování svého hlasu.

Interakce volič a kolektor: kolektor přijme podepsanou obálku s hlasem od voliče a ponechává si je.

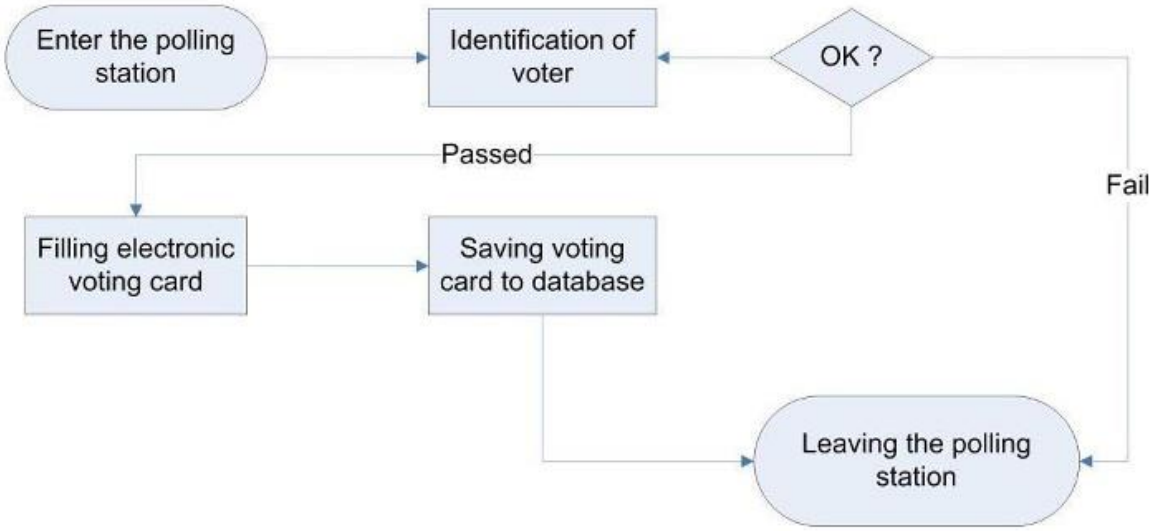
Kolektor: Veškeré kolektory po uplynutí voleb začnou sčítat obdržené obálky a umožní interpretaci a kontrolu výsledku voleb.

3.4 Technické řešení

Technické řešení elektronických voleb nabízí spoustu zajímavých řešení a umožňuje použití nových technologií. Tyto technologie se dají využít k identifikaci, uchovávaní dat nebo k interakci s uživatelem. Každá ze zemí Evropské unie, ale i ve světě, se k tomuto problému staví individuálně a dá se říct, že ještě nevznikl koncept platných norem, dle kterých by se musely řídit. V našem mladém demokratickém systému je zapotřebí takovéto zásadní změny provádět postupně a proto si představíme dvě základní řešení. První řešení je kompletní elektronizace papírové formy voleb. Ve druhém řešení se počítá s možností volby přes internet.

3.4.1 Elektronizace papírové formy

Elektronizace by měla nahradit veškeré papírové formuláře v procesu voleb, ovšem samotný průběh bude nezměněn. Volič navštíví volební místnost určenou dle jeho bydliště, tato volební místnost bude vybavena takzvanou „all-in“ sadou, která by měla zahrnovat dotykový display, identifikační technologii a potřebnou volební aplikaci. Pokud toto místo navštíví, bude nucen se u terminálu identifkovat například otiskem prstu nebo skenováním oční sítnice. Jestliže identifikace proběhne v pořádku, je volič připuštěn do aplikace a může zadat svojí volbu, odeslat hlas a následně opustit volební místnost.[8]



Obrázek 1: elektronický volební proces

Elektronický volební terminál

Elektronický volební termín by měl obsahovat základní komponenty, jako jsou procesor s integrovanou grafickou kartou, operační paměť, hard-disk, dotykový display, a operační systém Android, Linux nebo jiný.

Tzv. **„all-in“ sada:** tyto sady jsou vyráběny za účelem minimalizace velikosti zbavením se všech nepotřebných příslušenství, kdy veškeré potřebné komponenty jsou integrovány do jediného přístroje. Zmíněné terminály jsou na trhu dostupné po dobu již několika let a dle mého názoru a zkušeností se v praxi osvědčily, ať už při interakci s terminálem v obchodním centu, bance nebo na úřadu.

Obrázek 2: biometrický identifikační terminál

Identifikační technologie

U tohoto navrhovaného systému myslíme termínem identifikační technologie takovou technologii, která využívá biometrické údaje k identifikaci voliče. Tedy biometrické údaje člověka měřitelné a zjistitelné vícero způsoby, z nichž se v této práci budu zajímat zejména o následující:

I. Autentizace otisku prstu
II. Autentizace oční duhovky

Uvedené metody mají nespornou výhodu v porovnání s jinými identifikačními technologiemi v tom směru, že všichni občané, mají dané své unikátní příslušenství pro identifikaci od narození a není nutné, aby museli disponovat nějakým externím zařízením jako například čipovou kartou, samozřejmě až na výjimky občanů s určitým handicapem, kteří mají nárok na asistovanou volbu. Zmíněné identifikační technologie založené na porovnávání biometrických údajů jsou v mnoha směrech pohodlnější i bezpečnější.[9]

Autentizace otisku prstu

Jak už jsme již konstatovali, každý člověk na naší planetě po sobě zanechává unikátní otisky prstu a proto je to výborný prostředek k identifikaci, užívaný jak v kriminalistice, tak v běžné praxi pro otevírání dveří nebo přihlášení se k zařízení. Tento atribut je z hlediska funkčnosti zásadní. Tato metoda snímá přímý optický snímek otisku a ten následně porovná s národní databází a nalezne shodu. Jedná se o jednu z levnějších variant biometrické identifikace.[9]

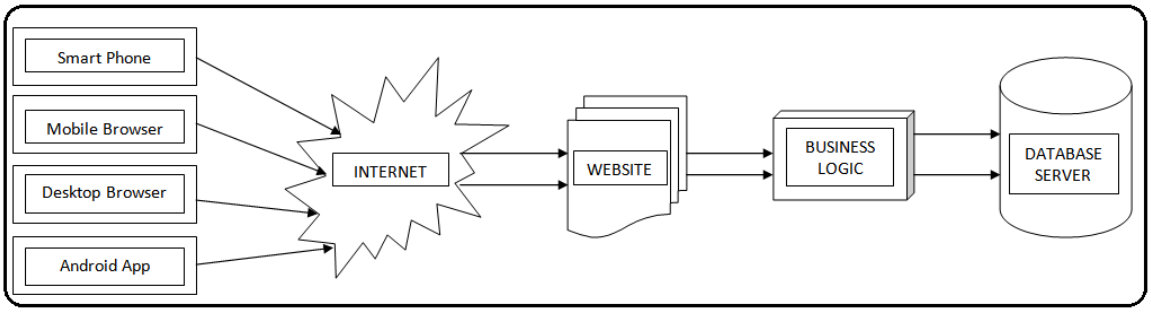
Autentizace oční duhovky

Metoda autentizace oční duhovky je založena na porovnávání přechodů zornice a duhovky a duhovky a bělma. Přechody snímá malý objektiv, který během několika sekund vytvoří soubor snímků a odešle jej k porovnání. Tato metoda díky své vysoké bezpečnosti a ceně není tak rozšířená ve společnosti, používá se spíše u identifikace přístupu zaměstnanců do farmaceutických laboratoří nebo jiných armádních, vládních a dalších vysoce zabezpečených prostor.[9]

3.4.2 Volby přes internet

Takovýto systém musí obsahovat internetovou stránku se zajištěnou kompatibilitou s jakýmkoliv internetovým prohlížečem na různých zařízeních, jako jsou laptopy, chytré telefony nebo stolní počítače. Interakce s internetovou stránkou může nastat pouze tehdy, pokud dané zařízení bude připojeno k internetu. Tento systém by mohl využívat například tří stupňovou architekturu (obrázek 3). Tří stupňová architektura využívá třech základních vrstev, kde první vrstva představuje internetovou stránku a zajišťuje autentičnost voliče a měla by zahrnovat následující základní údaje:

I. Přihlášení / Registraci
II. Hlasovací formulář
III. Listinu kandidátů
IV. Výsledky
V. Pomocné hlášení chyb
VI. Kontakty



Obrázek 3: Tří vrstvá architektura

Druhá vrstva je takzvaná pracovní vrstva, do které jsou posílány veškeré pracovní záležitosti z internetové stránky, od nutné registrace až po ověřování odeslaných hlasů. Pracovní vrstva musí spolupracovat s třetí databázovou vrstvou poskytující uložené informace ve chvíli, kdy je to zapotřebí.

Android nebo IOS aplikace by měla být taktéž propojená s první vrstvou stejně jako internetový prohlížeč zajišťující zobrazení internetové stránky. Aplikace by si měly pomocí skriptu vypůjčit obsah z první vrstvy a upravit si jej dle svých požadavků jako jsou například design nebo rozlišení. Hlavní kontext musí z hlediska bezpečnosti zůstat nezměněn. Úpravou designu nebo rozlišení lze dosáhnout plynulejšího pohybu mezi záložkami v aplikaci, což je jeden z vyžadovaných požadavků jak ze strany uživatelů, tak ze strany provozovatelů. Rychlost aplikace je také zásadní, a to nejenom v otázce bezpečnostního časového limitu volby samotné. Tento limit musí být stanoven dle komplexnosti voleb probíhajících (v případě voleb do Parlamentu České republiky bude časový limit pro volbu zajisté větší než v případě referenda, u kterého je zapotřebí zaškrtnout pouze checkbox s odpovědí ano/ne).[10]

4 Zkušenosti ze zahraničí

4.1 Elektronické volby v zahraničí

V této části své práce se zaměřím na realizované elektronické volby v zahraničí. Z veřejně dostupných zdrojů nasbírané informace mi pomohou k sestavení kritérií a k ohodnocení těchto systémů použitých v elektronických volbách. Za použití více kriteriální analýzy tyto systémy porovnám a výsledky této analýzy použiji za účelem intepretace závěru, který by měl obsahovat doporučená východiska pro Českou republiku. Ke správnému použití metody vícekriteriální analýzy je zapotřebí si stanovit následující:

I. Porovnávané státy a jejich systémy elektronických voleb
II. Kritéria systémů e-voleb
III. Ohodnocení jednotlivých systémů
IV. Váhy kritérií
V. Interpretace výsledku

4.2 Porovnávané státy a jejich systémy e-voleb

4.2.1 Estonsko

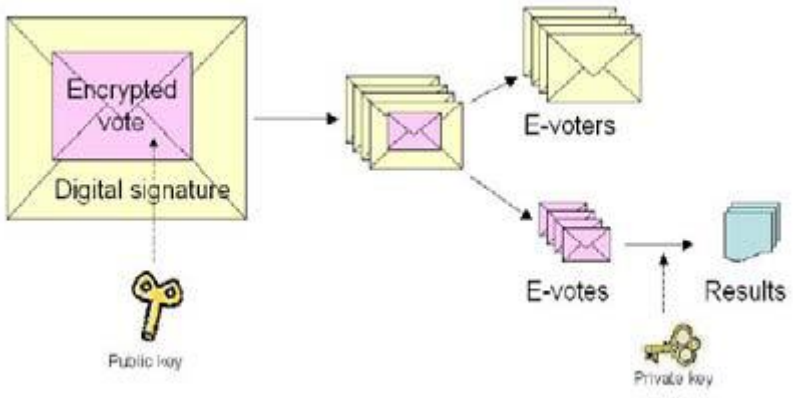
V Estonsku byl poprvé představen a použit systém e-voleb v roce 2005 a to ve volbách do městských zastupitelstev. V roce 2007 byl tento systém poprvé na světě použit při Parlamentních volbách. Cílem tohoto systému nebylo nahradit stávající volební proces, nýbrž jej rozšířit, zdokonalit a umožnit přístup k volbám bez nutnosti navštívit volební místnosti. Estonský systém e-voleb je založen a pevně spjat s ID kartou. Tato karta je vydávána občanům bez ohledu na to, zda občan chce nebo nechce volit skrze internet, popřípadě využívat i jiných služeb, které tato ID karta nabízí. Estonsko se také může pyšnit nejdelší zkušeností v tomto oboru, jelikož systém e-voleb provozuje více jak jedno desetiletí.

Struktura systému je tedy postavena na distribuci ID karet obsahujících dva PIN kódy. Kde první PIN kód identifikuje voliče při přihlášení do systému a druhý PIN kód

podepisuje obálku s hlasem v digitální formě. Pro zajištění legitimity voliče existuje databáze registrovaných voličů, kde jsou registrováni všichni občané Estonska. Samotný proces e-volby má následující kroky:

I. Navštívit internetovou stránku, která vyžaduje ID kartu voliče ve čtečce
II. Ověření identity voliče skrze první PIN kód
III. Následné ověření voliče a porovnání jeho údajů s databází registrovaných voličů
IV. Zobrazení přehledu kandidátek politických stran nebo subjektů
V. Možnost výběru kandidátů a vytvoření zašifrovaného hlasu
VI. Podepsání zašifrovaného hlasu pomocí druhého PIN kódu
VII. Sečtení hlasů poté, co jsou odstraněny digitální podpisy pro zachování anonymity

Tento systém garantuje, že nepřetrvává žádné spojení mezi voličem a jeho hlasem. Estonský model také umožňuje změnu vlastního hlasu a není tak limitován podmínkou že, každý volič může hlasovat pouze jednou.[11]



Obrázek 4: Estonský model

4.2.2 Švýcarsko

Ve Švýcarsku jsou známy tři základní metody voleb. První metoda je klasické navštívení volební místnosti s účastí okolo 10%. Druhá metoda je založená na velké důvěře občanů Švýcarska v jejich národní poštovní úřad, jelikož přibližně 70% voličů posílá své hlasy poštou. Třetí metodou možnosti volby je hlasování přes internet s účastí přibližně 20%. Před začátkem každých voleb voliči obdrží voličské průkazy, na které jsou nahrány jejich identifikační údaje. Volby druhou a třetí metodou jsou otevřeny z pravidla o pár dní dříve tak, aby odevzdané hlasy byly připraveny k sečtení v den ukončení hlasování.

Vzhledem ke skutečnosti, že ve Švýcarské federaci jsou rozdílné regionální politické systémy, bylo nutné vytvořit i tři rozdílné systémy e-voleb pro každý region zvlášť.

I. **Geneva systém** nabízí centralizované řešení, kde Ženeva je vývojářem a vlastníkem tohoto systému a také tento systém spravuje a provozuje.
II. **Zurich systém** je založen na decentralizovaném řešení. Kanton Zurich je vlastníkem i vývojářem tohoto systému, ale jako správce a provozovatel systému je určena externí soukromá společnost, jež zvítězí ve výběrovém řízení.
III. **Neuchâtel systém** stejně jako Ženevský systém nabízí centralizované řešení. Kanton je vlastníkem, správcem a provozovatelem tohoto systému, jenž byl ovšem vyvinut soukromou externí firmou, která vyhrála výběrové řízení za tímto účelem vypsané. Tento systém na rozdíl od předešlých výše zmíněných neumožňuje pouze internetové hlasovaní, ale má v sobě integrovány i další funkce, jako je možnost podání daňového přiznání přes internet.

Výše uvedené systémy jsou díky Švýcarské barvitosti obyvatelstva realizovány ve čtyřech úředních jazycích (Němčina, Francouzština, Italština a Rétorománský jazyk).[12]

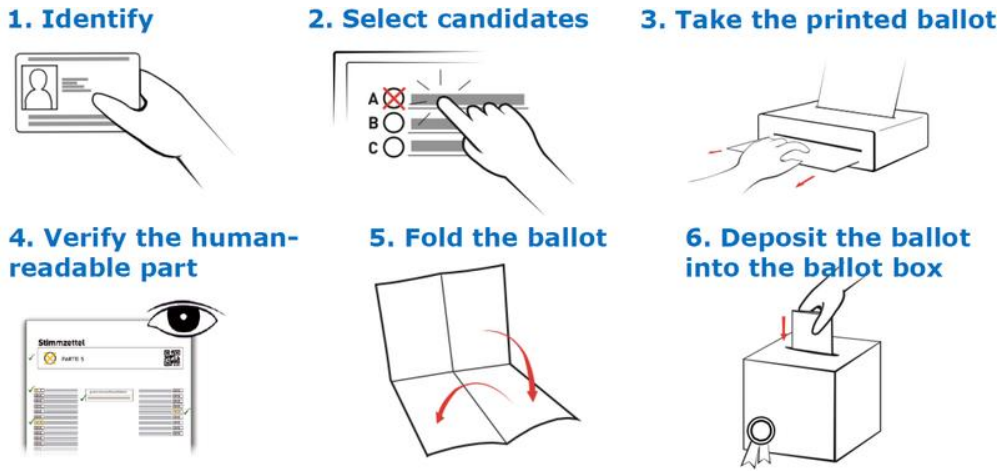
4.2.3 Německo

Německo uspořádalo první elektronické volby v roce 1999 za použití elektronických teminálů ESD1 a ESD2, které byly vyrobeny Holandskou společností Nedap. Problém těchto přístrojů je, že jsou to komerční produkty a jejich struktura tak není otevřena veřejnosti, což má za následky nedostatečnou transparentnost těchto přístrojů, v důsledku čehož bylo podáno mnoho žalob, v nichž byla namítána právě nedostatečná transparentnost a následná možnost kontroly voleb. Německá vláda se z tohoto důvodu rozhodla tyto terminály nadále nepoužívat, jelikož byly shledány jako protiprávní a rozhodla se vyvinout vlastní moderní bezpečný systém e-voleb s názvem EasyVote.

EasyVote je hybridní elektronický systém založený na částečné elektronizaci volebního procesu za využití hlasovacího terminálu, tiskárny a čtečky QR kódu. Tento proces se nějak významně neliší od papírové formy, avšak pár odlišností přece jenom obsahuje.[13]

Proces volby systému EasyVote má následující kroky:

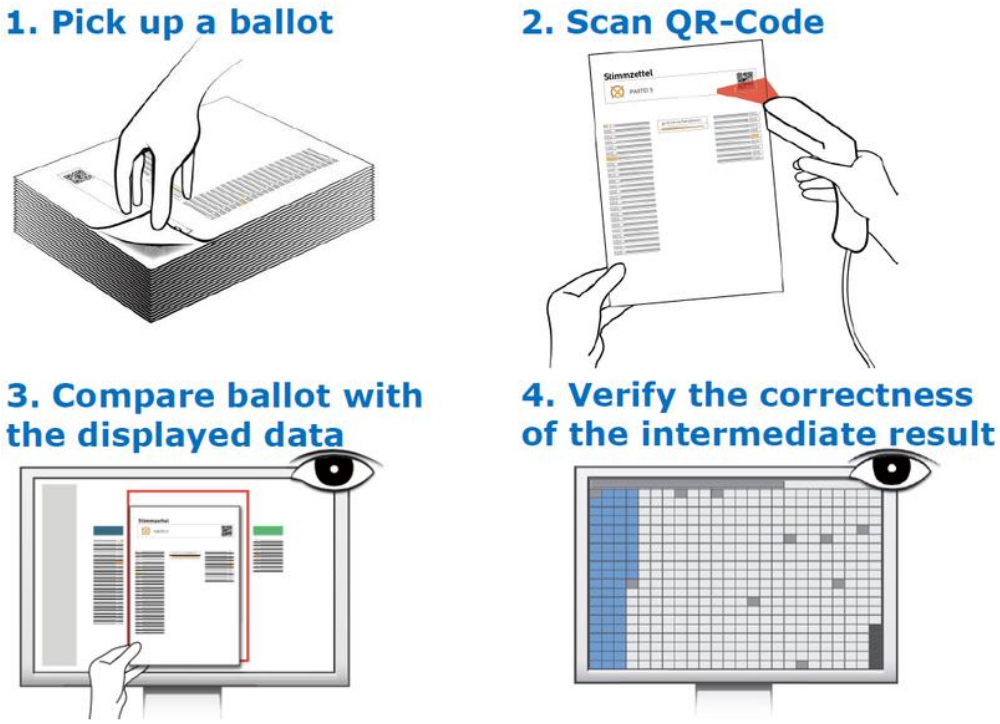
I. Identifikace voliče personálem volební místnosti za použití ID karty a jmenného seznamu
II. Volič je vpuštěn k terminálu, ke kterému se také přihlásí prostřednictvím ID karty a následně vybere svého kandidáta
III. Terminál odešle hlas do databáze a automaticky vytiskne hlas voliče pro jeho vizuální kontrolu
IV. V případě, že je vše v naprostém pořádku, volič svůj hlas přeloží a vhodí jej do urny



Obrázek 5: Průběh voleb v systému EasyVote

Proces sčítání hlasů v systému EasyVote probíhá následovně:

I. Personál volebních místností otevře zapečetěnou urnu s hlasy
II. Z každého odevzdaného hlasu naskenuje QR kód pro spárování s hlasem v databázi
III. Každý hlas je vizuálně porovnán personálem s hlasem v databázi
IV. Pokud je vše v pořádku pracovník hlas potvrdí jako platný



Obrázek 6: Sčítací proces systému EasyVote

4.2.4 Spojené království Velké Británie a Severního Irska

Spojené království, ve snaze zvýšit volební účast v celé zemi, umožňuje autoritám zavádění nových zkušebních metod účasti ve volbách. Je nutné konstatovat, že všechny tyto metody nebyly započteny do výsledku voleb. Těchto metod je celkem pět a jsou to volby přes internet, mobilní telefon, digitální televizi, SMS a elektronický terminál.

Volby přes internet ve Spojeném Království jsou realizovány tak, že každý oprávněný volič obdrží volební kartu, na které je uvedeno ID voliče a heslo potřebné za účelem přihlášení do systému na internetových stránkách.

Volby prostřednictvím elektronických terminálů, téměř identické Belgickému modelu, probíhají tak, že identifikaci voliče zajišťuje personál hlasovacích místností. Volič po úspěšné identifikaci obdrží chytrou volební kartu umožňující přihlášení k elektronickému terminálu a úspěšné odeslání hlasu. Poté volič chytrou volební kartu předá personálu volebních místností, který obsah této karty přes čtečku nahraje do systému a v případě schody hlas započte.

Volby za použití mobilního telefonu probíhají tak, že volič zavolá na bezplatnou linku a během hovoru zadá číselný kód svého kandidáta, jenž nalezne na volební kartě. Po zadání tohoto kódu systém automaticky přečte jméno tohoto kandidáta a volič jej potvrdí.

Hlasování za použití SMS zprávy se uskuteční tak, že volič odešle mobilní zprávu v předepsaném tvaru a s údaji uvedenými na volební kartě včetně čísla kandidáta a ochranného kódu. V případě, že je zpráva odeslána ve správném tvaru, volič obratem obdrží potvrzení o započtení hlasu.

Volby přes digitální televizi. Volič se prostřednictvím teletextu nebo případně HbbTv aplikace přihlásí do systému s údaji z volební karty pro jeho identifikaci. Po úspěšném přihlášení je volič schopen vybrat si v seznamu svého kandidáta a odeslat hlas.[14]

4.2.5 Belgie

Belgická vláda v roce 1992 vypracovala analytickou studii, jejímž cílem byl výběr nejlepšího elektronického volebního systému pro celou zemi. Výsledky této studie ukázaly na dva vhodné systémy, jejichž názvy jsou DIGIVOTE-systém a JITES-systém. Každá obec se tak mohla sama rozhodnout, jaký z těchto dvou systémů bude uplatňovat při volbách.

Den před zahájením voleb, každý předseda jednotlivých hlasovacích místností obdrží dvě obálky. První obálka obsahuje unikátní heslo pro konkrétní volební místnost. Druhá obálka obsahuje speciální disk, jímž se aktivují elektronické volební terminály. Kombinace těchto dvou prvků generuje šifrovací klíč zaměřený na zachování integrity softwaru a dat v terminálech.[15]

Samotný proces volby je následovný:

- Aktivace terminálu pomocí bootovacího disku
- Zadání hesla pro aktivaci magnetických karet předsedou volební místnosti
- Bootovací disk se následně připojí k elektronickému obálkovému boxu
- Přenos hlasů z magnetických karet do elektronického obálkového box a vytvoření zálohy na bootovací disk
- Volič obdrží magnetickou kartu, která obsahuje registrovaný hlas voliče
- Volič vybere svého kandidáta po přihlášení se kartou k terminálu
- Navrácení magnetické karty personálu volební místnosti
- Vložení magnetické karty do elektronického obálkového boxu
- Uložení hlasu voliče z magnetické karty do bootovacího disku přes čtečku karet
- Porovnání čísla voliče v obálkovém boxu s číslem voliče na magnetické kartě
- Vypnutí elektronického terminálu předsedou volební místnosti po skončení voleb
- Uchování magnetické karty v zapečetěném obálkovém boxu až do oznámení platnosti voleb (pokud ne je obálkový box otevřen pro potřebnou kontrolu hlasů)
- Předseda předá zapečetěnou obálku s bootovacím diskem a zálohou příslušným autoritám

- Předseda vloží bootovací disk do počítače příslušných autorit k sečtení výsledků voleb (v případě problému s diskem je použita záloha)
- V případě, že disk i záloha jsou nepoužitelné, je elektronický obálkový box podroben expertíze za účelem zjištění stavu hlasů

4.3 Analýza systému e-voleb v zahraničí

Tato část práce se zaměřuje na metodu vícekriteriálního porovnání systémů e-voleb výše zmíněných evropských států. Tabulky 1-12 ukazují průběh a výsledky této analýzy. Výchozí kritéria pro porovnání metodou vícekriteriálního rozhodování jsem stanovil takto:

I. Bezpečnostní prvky
II. Použité technologie
III. Možnosti přístupu
IV. Identifikace e-ID kartou
V. Rok zavedení
VI. Reálné užití

Dílčí části jsou ohodnocení systému, kvantifikace ohodnocených systému, dominance variant, určení vah kritérií, porovnání jednotlivých kritérii a výsledky analýzy. Ohodnocení kritérií systému e-voleb je stanoveno dle zjištěných informací o systémech jednotlivých evropských států. [11] [12] [13] [14] [15]

4.4 Ohodnocení jednotlivých systému

4.4.1 Porovnání systému e-voleb v zahraničí

Kritérium / Země	E-volby ze zahraničí	Použité technologie	Možnosti přístupu	Identifikace e-ID kartou	Rok zavedení	Reálné užití
Estonsko	NE	IA, DP, ŠO	osobně, internet	ANO	2005	aktivní
Belgie	NE	EVM	osobně	NE	1994	aktivní
Švýcarsko	ANO	IA	osobně, internet	NE	2001	aktivní
UK	NE	IA,SMS,EVM	osobně internet	NE		neaktivní
Německo	NE	EVM	osobně	NE		neaktivní

Tabulka 1: Stanovení kritérií a ohodnocení systémů

4.4.2 Kvantifikace a charakter kritérií

Kritérium / Země	E-volby ze zahraničí (body)	Použité technologie (body)	Možnosti přístupu (body)	Identifikace e-ID kartou (body)	Rok zavedení (pořadí)	Reálné užití (body)
Estonsko	0	9	5	5	3	10
Belgie	0	5	3	0	1	10
Švýcarsko	5	7	5	0	2	10
UK	0	8	5	0		0
Německo	0	5	3	0		0
Povaha krit.	MAX	MAX	MAX	MAX	MIN	MAX

Tabulka 2: Kvantifikace ohodnocených systémů

4.4.3 Dominance alternativ

Kritérium / Země	E-volby ze zahraničí (body)	Použité technologie (body)	Možnosti přístupu (body)	Identifikace e-ID kartou (body)	Rok zavedení (pořadí)	Reálné užití (body)
Estonsko	0	9	5	5	3	10
Belgie	0	5	3	0	1	10
Švýcarsko	5	7	5	0	2	10
UK	0	8	5	0		0
Německo	0	5	3	0		0

Tabulka 3: Dominance Estonska

4.4.4 Úprava matice po odstranění dominance

Kritérium / Země	E-volby ze zahraničí (body)	Použité technologie (body)	Možnosti přístupu (body)	Identifikace e-ID kartou (body)	Rok zavedení (pořadí)	Reálné užití (body)
Estonsko	0	9	5	5	3	10
Belgie	0	5	3	0	1	10
Švýcarsko	5	7	5	0	2	10
Povaha krit.	MAX	MAX	MAX	MAX	MIN	MAX

Tabulka 4: Výchozí model pro porovnání

4.5 Váhy kritérií dle Saatyho párového porovnání

Kritérium	E-volby ze zahraničí	Použité technologie	Možnosti přístupu	Identifikace e-ID kartou	Rok zavedení	Reálné užití	**bj**	**vj**
E-volby ze zahraničí	1	1/5	1/3	1/7	3	1/9	0.2374	**0.0111**
Použité technologie	5	1	1/3	5	3	1/9	1.2910	**0.0605**
Možnosti přístupu	3	3	1	7	5	1/9	2.4323	**0.1139**
Identifikace e-ID kartou	7	1/5	7	1	7	1/9	1.6616	**0.0778**
Rok zavedení	1/3	1/3	1/5	1/7	1	1/9	0.1370	**0.0064**
Reálné užití	9	9	9	9	9	1	15.5885	**0.7302**
						SUMA	21.3477	

Tabulka 5: Určení vah kritérií

4.6 Párové porovnání alternativ z hlediska jednotlivých

4.6.1 E-volby ze zahraničí

E-volby ze zahraničí	0.0111	Estonsko	Belgie	Švýcarsko	Ri		vi
	Estonsko	1	1	1/9	0.5774	0.1390	**0.0015**
	Belgie	1	1	1/9	0.5774	0.1390	**0.0015**
	Švýcarsko	9	9	1	3.0000	0.7221	**0.0080**
					4.1547	1	**0.0111**

Tabulka 6: Porovnání 1. kritéria

4.6.2 Použité technologie

Použité technologie	0.0605	Estonsko	Belgie	Švýcarsko	Ri		vi
	Estonsko	1	7	3	2.1407	0.5152	**0.0057**
	Belgie	1/7	1	1/5	0.4111	0.0990	**0.0011**
	Švýcarsko	1/3	5	1	1.1362	0.2735	**0.0030**
					3.6880	0.887680855	**0.0099**

Tabulka 7: Porovnání 2. kritéria

4.6.3 Možnosti přístupu

Možnosti přístupu	0.1139	Estonsko	Belgie	Švýcarsko	Ri		vi
	Estonsko	1	3	1	1.3161	0.3168	**0.0035**
	Belgie	1/3	1	1/3	0.5774	0.1390	**0.0015**
	Švýcarsko	1	3	1	1.3161	0.3168	**0.0035**
					3.2095	0.772498106	**0.0086**

Tabulka 8: Porovnání 3. kritéria

4.6.4 Identifikace e-ID kartou

Identifikace e-ID kartou	0.0778	Estonsko	Belgie	Švýcarsko	Ri		vi
	Estonsko	1	5	5	2.2361	0.5382	**0.0060**
	Belgie	1/5	1	1	0.6687	0.1610	**0.0018**
	Švýcarsko	1/5	1	1	0.6687	0.1610	**0.0018**
					3.5735	0.86012182	**0.0096**

Tabulka 9: Porovnání 4. kritéria

4.6.5 Rok zavedení

Rok zavedení	0.0064	Estonsko	Belgie	Švýcarsko	Ri		vi
	Estonsko	1	1/7	1/3	0.4671	0.1124	**0.0013**
	Belgie	7	1	5	2.4323	0.5854	**0.0065**
	Švýcarsko	3	1	1	1.3161	0.3168	**0.0035**
					4.2155	1.01463661	**0.0113**

Tabulka 10: Porovnání 5. kritéria

4.6.6 Reálné užití

Reálné užití	0.7302	Estonsko	Belgie	Švýcarsko	Ri		vi
	Estonsko	1	1	1	1.0000	0.2407	**0.0027**
	Belgie	1	1	1	1.0000	0.2407	**0.0027**
	Švýcarsko	1	1	1	1.0000	0.2407	**0.0027**
					3.0000	0.722073702	**0.0080**

Tabulka 11: porovnání 6. kritéria

4.7 Výsledek analýzy vícekriteriálního rozhodování

Stát	vi	Pořadí
Estonsko	0.02070721	**2**
Belgie	0.015166112	**3**
Švýcarsko	0.02258002	**1**

Tabulka 12: Výsledná tabulka porovnání

Dle analýzy párového porovnání stanovených kritérií jednotlivých systémů, vyšel jako nejlepší Švýcarský model. Hned poté následoval Estonský model, který v této analýze skončil v těsném závěsu za Švýcarským modelem. Třetí se umístil belgický systém.

5 Diskuse

Musíme si položit otázku, jaké přínosy bude mít tato analýza pro Českou republiku? Je zřejmé, že přínosy budou spočívat zejména v uvědomění si přínosu elektronizace volebního procesu, barvitosti možných řešení elektronizace a použitelnosti nových technologií, které jsou pro voliče přitažlivé a přináší požadovaný komfort.
Česká republika je v dobré pozici pro realizaci elektronizace volebních procesů. Tato pozice je zejména dána možností studia bohatých zkušeností ze zahraničí.

Je Česká republika schopná provozně technicky zabezpečit průběh e-voleb?
Ano, Český statistický úřad (ČSÚ) je v dobré kondici, pozici a technologické vybavenosti, a tudíž by měl být schopen zvládat přijímat, uschovávat, ověřovat a interpretovat výsledky přijatých hlasů. Elektronický systém voleb by měl realizovat i provozovat například kraj aby se tak rozložila působnost těchto systémů. Realizátor by měl v případě realizace využít stávajícího registru osob a v úvahu systému datových schránek (například pro doručování elektronických klíčů).

Je pro Českou republiku vhodnější centralizované nebo decentralizované řešení?
Z výše uvedeného analýzy je jasné, že centralizované řešení státem pod záštitou ČSÚ a Ministerstva vnitra je méně vhodné. A to z důvodů většího rizika napadení volebního systému. Naopak decentralizované systémy jsou díky svému rozložení působnosti méně atraktivní k napadení a i v případě napadení neobsahují kompletní data a chrání je tak před zneužitím.

Jak by měla Česká republika postupovat?
Postup by mohl být následovný. Česká republika by se prvně zaměřila na volby přes internet. Vytvořila by tak velice zajímavé a komfortní prostředí pro voliče. Tyto systémy by se měly před zavedením důkladně otestovat a měly by je doprovázet tzv. „ostré testy“

na méně náročných volebních procesech jako jsou například referenda. Další kroky jsou přímo závislé na výsledcích zavedení voleb přes internet. Je otázkou, zda zachovat klasickou papírovou formu voleb jako alternativu, nebo jestli přistoupit k celkové elektronizaci volebního procesu zahrnující elektronické volební terminály.

Mělo by zavedení e-voleb v České republice za následek zvýšení volební účasti? Zkušenosti z jiných evropských zemí ukazují, že volební účast po zavedení e-voleb má tendenci stoupat. Zvyšovat se bude postupně, tudíž nemůžeme očekávat jednorázový skokový nárůst v jednotkách procent.

6 Závěr

Elektronické volby jsou v dnešní moderní době jasným krokem vpřed a posunují vývoj e-Goernmentu k úplné elektronizaci státní správy o znatelnou část dál.

Standardy a principy e-voleb jsou zajištěny kombinací kryptografických šifer a bezpečných procesů. Kryptografické šifry v systémech zabezpečují zejména soukromí, férovost a ověření. Bezpečné procesy se zabývají interakcí člověka se systémem a zaručují tak jeho bezpečnost a současně transparentnost hlasování. Navrhovaný model využívá kombinace šifer blind signature, secret sharing a pseudo random generator. V úvahu připadají dva základní modely realizace uvedených voleních systémů. První model ponechává stávající průběh volebního procesu, ale nahrazuje veškeré papírové prvky elektronickými prvky. Druhy model využívá webové aplikace komunikující s různými chytrými zařízeními přes internet a umožňuje tak uživateli přihlášení z různých míst a prostředí.

Analýza elektronických volebních systémů v zahraničí zahrnuje získané poznatky o zkoumaných systémech a porovnává je. Vybrané zahraniční systémy jsou Estonský, Švýcarský, Německý, Belgický a Spojeného království. Výsledky vícekriteriální analýzy nám jasně udávají, že druhý model zahrnující volby přes internet je v zahraničí silněji preferován než model elektronizace papírové formy. Také udává, který z těchto systémů vzešel jako celkový vítěz. Nejlepších výsledků dosáhlo Švýcarsko s decentralizovaným

systémem e-voleb, kdy tento systém je aplikován z důvodu rozdílné legislativy jednotlivých regionů. S minimálním rozdílem skončilo Estonsko s centralizovaným systémem voleb, kde je použití centralizovaného systému logické vzhledem k jednotnému právnímu řádu a velikosti Estonska.

Nutná východiska pro zavedení e-voleb v České republice jsou definována podle navržených modelů e-voleb a výsledků analýzy. Dle zjištěných informací by se měla Česká republika ubírat spíše směrem decentralizovanému systému e-voleb. Decentralizované systémy jsou bezpečnější díky své rozložené působnosti a taktéž nikdy neobsahují kompletní data. Dalším možným východiskem pro Českou republiku je nepochybně zavedení internetového volebního systému, jenž by zajistil z pohledu uživatele požadovanou atraktivitu a komfort. Uživatelská atraktivita a komfort se podle zkušeností ze zahraničí projevují postupným zvyšováním volební účasti.

7 Seznam použitých zdrojů

[1] Nález Ústavního soudu České republiky Pl.ÚS 25/96 ze dne 2. 4. 1997

[2] Zákon č. 275/2012 Sb., o volbě prezidenta republiky a změně některých zákonů

[3] Referendum: czso [online]. 2016 [cit. 2016-03-04]. Dostupné z: https://www.czso.cz/csu/czso/pusobnost_csu_ve_volbach_a_v_referendu

[4] Singh, N. & Das, S. 2014, "Cryptanalysis of Blind Signature Schemes", International Journal of Computer Science and Network Security (IJCSNS), vol. 14, no. 5, s. 73. ISSN:1738-7906

[5] Shamos, M. & Yasinsac, A. 2012, "Realities of E-voting Security", *IEEE Security & Privacy*, vol. 10, no. 5, s. 16-17. ISSN:1540-7993

[6] Hillery, M., Buzek, V. & Berthiaume, A. 1998, "Quantum secret sharing". ISSN:1570-0755

[7] Avaroğlu, E., Koyuncu, İ., Özer, A.B. & Türk, M. 2015, "Hybrid pseudo-random number generator for cryptographic systems",*Nonlinear Dynamics*, ISSN:0924-090X

[8] Šilhavý, R. 2011, Computer science and software techniques in 2011, Šilhavý, Vsetín. ISBN:9788090474109

[9] Jain, A.K. & Nandakumar, K. 2012, "Biometric Authentication: System Security and User Privacy", *Computer*, vol. 45, no. 11, s. 87-92. ISSN:0018-9162

[10] Kulkarni, V.A., Devraj, M., Chauhan, A., Pandey, A. & Chavan, S. 2015, "e-Voting System Using Android And Web-Based Platform", *International Journal of Advanced Research in Computer Science*, vol. 6, no. 1. e-ISSN:0976-5697

[11] Tsahkna, A. 2013, "E-voting: lessons from Estonia", *European View*, vol. 12, no. 1, s. 59-66. ISSN:1781-6858

[12] Beroggi, G.E.G. 2008, "Secure and Easy Internet Voting",*Computer*, vol. 41, no. 2, s. 52-56. ISSN:0018-9162

[13] EasyVote - An hybrid (electronic/paper) voting systém. EasyVote [online]. 2016 [cit. 2016-03-04] Dostupné z: https://www.secuso.informatik.tu-darmstadt.de/en/secuso-home/research/results/easyvote/

[14] Haren, R.v. & Pieters, W. 2007, "Temptations of turnout and modernisation: e-voting discourses in the UK and the Netherlands", *Journal of Information, Communication and Ethics in Society*, vol. 5, no. 4, s. 276-292. ISSN:1477-996X

[15] De Cock, D. & Preneel, B. 2007, "Electronic Voting in Belgium: Past and Future" in Springer Berlin Heidelberg, Berlin, Heidelberg, s. 76-87. ISBN:9783540774921
[16] Gerloch, A., Hřebejk, J., Zoubek, V.: Ústavní systém České republiky. 4. vydání. Praha: PROSPEKTRUM, 2010, s.122-127. ISBN 9788071751069
[17] Zákon č. 1/1993 Sb., Ústava České republiky, zákon č. 2/1993 Sb., Listina základních práv a svobod,
[18] Pavlíček V. a kolektiv: Ústavní právo a státověda, II. Díl. Ústavní právo České republiky. 1 úplné vydání. Praha: Leges, 2011, s. 437-447 ISBN 9788087212905